基于云计算的数据安全存储与访问控制技术研究

虞培培
宝武装备智能科技有限公司　上海市　201999

摘　要：随着云计算技术的飞速进步，大量数据依赖于云计算平台进行存储和访问，数据安全问题日益突出。本文深入探讨了基于云计算的数据安全存储与访问控制技术，首先阐述了数据安全的核心概念，随后探讨了在云计算环境下数据面临的安全挑战，并对相应的存储与访问控制策略进行了详细研究。本研究旨在确保数据在云计算环境中的保密性、完整性和可用性，以促进云计算产业的健康和可持续发展。

关键词：云计算；数据安全；存储技术；访问控制

1. 引言

云计算作为一种新兴的计算模式，凭借其强大的计算能力、灵活的资源配置和便捷的服务交付方式，在各个领域得到了广泛的应用和迅速的发展。越来越多的企业和个人将数据存储和业务处理迁移到云端，享受云计算带来的高效和便利。然而，随着数据在云端的集中存储和处理，数据安全面临着前所未有的挑战。数据泄露、篡改、丢失等安全事件频发，不仅会给用户带来巨大的经济损失和隐私泄露风险，也会对云计算服务提供商的声誉造成严重影响。因此，研究云计算环境下的数据安全存储与访问控制技术具有至关重要的现实意义。

2. 数据安全概念

在数字化时代，数据成为关键资产，影响社会各领域。企业利用数据优化决策、拓展市场；政府通过数据实现精准管理、提升公共服务。个人生活因数据融入而变得高效。数据安全，涉及保密性、完整性和可用性三大要素。

数据保密性侧重于防止内部信息外流。通过精细的身份认证机制，如多因素认证，结合内部网络隔离等手段，确保只有被明确许可的员工才能触及核心数据，像是企业研发的未公开技术资料、财务报表等敏感信息，被牢牢锁在私有云的 “安全屋” 内，避免商业机密被竞争对手窃取，维护企业的核心竞争力。完整性上数据的准确性、一致性不容有失。企业依靠严格的访问日志记录与定期的数据校验流程，随时监测数据在存储、传输以及内部共享环节有无被无意或蓄意篡改。以制造业企业为例，产品设计图纸、生产工艺参数等关键数据，必须保证从设计部门到生产车间流转过程中的完整性，否则错误数据引发的生产偏差将带来巨大损失。可用性而言，需保障内部业务顺畅运行，数据随时可供合法使用者高效调取。一方面，凭借冗余的硬件架构，即便部分服务器突发故障，数据依然能迅速切换至备用节点提供服务。另一方面，专业的运维团队时刻监控网络带宽、存储容量等资源，确保在业务高峰，如电商企业的促销活动、金融机构的结算时段，数据访问如丝般顺滑，员工与业务系统交互毫无阻碍，推动企业内部运营高效有序开展。

3. 云计算环境下数据面临的安全挑战

在云计算环境蓬勃兴起的当下，尽管其为企业数据管理带来诸多便利，然而数据面临的安全挑战也不容小觑。内部人员风险是首要问题，因为企业主要对员工开放。如果员工安全意识不强，例如随意共享账号密码或在不安全网络环境下访问私有云，可能会导致数据泄露。此外，有恶意的内部人员可能会蓄意窃取数据，由于他们了解内部架构和权限设置，可能造成企业核心商业机密外泄。系统架构和运维漏洞可能带来风险。私有云虽独立，但架构设计缺陷易受攻击，如 DDoS 可瘫痪网络。运维失误，如软件更新不及时，可能使系统暴露于安全漏洞，给黑客篡改或破坏数据的机会。数据存储与备份环节存在显著问题。存储设备故障可能导致数据丢失，即使有冗余设计，若备份策略不当，如备份频率低、数据完整性校验缺失，突发灾难时难以快速恢复完整数据，影响企业运营。存储介质老化、损坏也可能导致数据损坏，影响业务支持。不同行业、地区对数据安全有各异的法规政策要求，企业云计算环境必须确保满足这些标准，从数据分类存储、访问记录留存到跨境传输限制等诸多方面，稍有不

慎就可能面临法律风险，给企业声誉与运营带来负面影响。

4. 云计算数据安全存储技术

4.1 加密技术

为应对内部人员泄露与外部潜在攻击风险，采用多层次加密策略。在数据进入云存储前，先利用对称加密算法对数据进行快速加密，保障数据传输过程的保密性。存储于云端时，再结合非对称加密算法，用公钥加密对称密钥，进一步强化安全性，确保即使存储介质泄露，数据内容也难以被破解。针对不同敏感度的数据，实施分类加密。例如企业的核心技术文档采用高强度加密算法，而一般性办公文件采用相对常规的加密方式，既保障关键数据安全，又优化加密资源使用效率。还可以采用同态加密形式，允许对密文进行特定的运算，运算结果解密后与在明文上进行相同运算的结果一致。这使得数据可以在加密状态下进行处理，有效保护了数据的隐私。例如微软的 Azure 云计算平台在一些数据分析服务中尝试应用同态加密技术。企业客户可以将加密后的数据上传到 Azure 云，云端服务器利用同态加密算法对加密数据进行统计分析等操作，而无需解密数据，从而降低了数据泄露的风险，同时也满足了企业对数据隐私保护和数据分析的双重需求。

4.2 冗余存储技术

首先可以构建冗余存储架构，采用分布式存储技术，将数据分散存储在多个节点上，通过分布式算法来管理数据的存储和访问。这种方式提高了数据的可用性和可靠性，同时具备良好的扩展性。Ceph 广泛应用于科研机构存储大量数据。例如在天文学研究中，观测产生的大量天文图像数据存储在基于 Ceph 的分布式文件系统。Ceph 利用 CRUSH 算法均匀分布数据至多个节点，确保快速数据访问和高可用性，即使部分节点故障，也能保证数据访问，满足科研对大规模数据存储和高效访问的需求。

其次利用纠删码技术，通过分割数据并添加冗余信息来实现容错和数据恢复，相比传统复制冗余，它能显著降低存储成本。例如谷歌云存储使用此技术，将数据分割成多个块并生成冗余块，分散存储在多个节点。即使部分数据丢失，只要有超过一半的块存在，就能恢复原始数据，从而节省空间并降低成本。最后可以制定智能备份策略，依据数据重要性与更新频率动态调整备份周期。同时引入备份数据完整性校验机制，定期比对备份数据与源数据，确保备份数据可靠可用，在灾难发生时能迅速恢复业务。

5. 云计算访问控制技术

5.1 基于身份的访问控制

基于身份的访问控制通过用户的身份标识（如用户名、数字证书等）来决定其对资源的访问权限。系统依据预定义的策略进行用户认证和授权，实现对单个用户的精细控制。例如，在企业云计算系统中，员工凭账号登录，系统根据其身份信息和权限设置决定访问权限。软件开发公司的代码仓库存储在云端，只有认证并授权的开发人员才能访问相应代码模块，防止未授权访问，保护知识产权安全。这种访问控制适用于用户数量较少、身份明确且稳定的环境，如企业办公系统、政府信息管理系统等。在这些场景中，用户身份和权限配置固定，能有效保障数据安全和保密性。

5.2 基于角色的访问控制

基于角色的访问控制将用户划分为不同的角色，每个角色被赋予相应的权限，用户通过担任特定的角色来获得对资源的访问权限。例如在一个医院的云计算医疗信息系统中，医生、护士、管理员等角色被定义，医生角色具有查看和修改患者病历的权限，护士角色具有查看患者基本信息和护理记录的权限，管理员角色则负责系统的配置和维护等权限。当一位医生登录系统时，系统根据其医生角色赋予相应的病历访问和修改权限，使其能够正常开展医疗工作，同时避免了护士或其他非医生角色对病历的不当操作，保障了医疗数据的安全和规范使用。

优势在于简化了访问控制的管理，当用户的角色发生变化时，只需修改其角色对应的权限，而无需逐个修改用户的访问权限，提高了管理效率。局限性在于角色的定义可能不够灵活，无法满足一些复杂的权限管理需求，例如在某些情况下，同一个用户可能需要在不同的情境下具有不同的权限，而基于角色的访问控制可能难以实现这种细粒度的权限分配。

5.3 基于属性的访问控制

基于属性的访问控制使用用户、资源和环境等多个属性来决定访问权限。用户属性可以包括职位、部门、年龄等，资源属性可以包括数据的敏感程度、所属项目等，环境属性可以包括时间、地点、网络条件等。系统根据这些属性制定访问策略，只有当用户的属性满足资源的访问条件时，才允许其访问。例如在一个金融机构的云计算系统中，只有在工作时间内，且用户属于风险管理部门，并且访问的是低风险

级别的金融数据时，才允许其进行读取操作。这样可以根据金融数据的敏感性和风险级别，以及用户的工作职能和时间等属性，灵活地控制数据的访问权限，防止内部人员在非工作时间或越权访问敏感数据，有效降低了数据泄露的风险。ABAC 的灵活性体现在它能够根据各种复杂的属性组合来制定精细的访问策略，适应不同的业务需求和安全场景。然而，这种灵活性也带来了一定的复杂性，包括属性的管理、访问策略的制定和维护等方面都需要较高的技术水平和管理成本。

5.4 访问控制技术的扩展与融合

为了充分发挥不同访问控制技术的优势，一些混合访问控制模型被提出。例如，将基于角色的访问控制和基于属性的访问控制相结合，先根据用户的角色进行初步的权限分配，然后再根据用户和资源的属性进行进一步的细粒度权限调整。在一个大型企业的云计算资源管理系统中，对于一般员工，先根据其所在部门和职位赋予相应的角色权限，如市场部员工具有访问市场推广资料的角色权限。然后再根据具体的资源属性，如某些特定市场调研报告的敏感级别和所属项目，结合员工的个人属性，如是否参与该项目等，进一步细化其对这些资源的访问权限。这种混合模型在一定程度上弥补了单一访问控制技术的不足，提高了访问控制的灵活性和适应性。访问控制技术还可以与其他安全技术如身份认证、审计等进行集成，形成一个完整的安全防护体系。例如在用户进行访问请求时，首先通过多因素身份认证技术对用户的身份进行严格验证，如密码、短信验证码、指纹识别等多种方式结合，然后访问控制系统根据用户的身份和权限进行访问决策，同时审计系统对用户的访问行为进行记录和分析，以便在发生安全事件时能够进行追溯和调查。某互联网金融平台采用了这种集成方式，用户在登录时需要通过密码和短信验证码进行身份认证，登录后访问控制模块根据用户的权限决定其可操作的功能和范围，同时审计系统记录用户的每一次操作，包括操作时间、操作内容等信息。一旦发生异常操作，如大量资金异常转移等情况，审计系统能够快速提供详细的操作记录，帮助平台及时发现和处理安全问题，保障用户的资金安全和平台的稳定运行。

6. 数据安全存储与访问控制技术整合的优势与挑战

优势

通过整合数据安全存储和访问控制技术，可以实现全方位、多层次的数据安全防护。不同技术之间相互补充和协同工作，能够应对各种复杂的安全威胁和业务需求。例如加密技术保护数据的机密性，冗余存储技术保证数据的可用性，访问控制技术防止未经授权的访问，从而提高了数据的整体安全性和可靠性。

挑战

技术整合也面临一些挑战，如不同技术之间的兼容性问题、系统性能的影响以及管理复杂度的增加等。例如，在将多种加密算法和存储技术集成时，可能会出现加密后的数据格式与存储系统不兼容的情况，需要进行额外的转换和适配工作。同时过多的安全技术叠加可能会对系统的性能产生一定的影响，需要在安全性和性能之间进行平衡。此外综合管理多种安全技术也需要专业的技术人员和完善的管理流程，增加了管理的难度和成本。

结论

总之，保障云计算环境下的数据安全是一个持续发展和不断演进的过程，需要不断地进行技术创新和实践探索，未来的研究可以关注以下几个方向：一是量子计算对传统加密技术的影响及新型量子安全加密技术的研究；二是针对边缘计算与云计算融合场景下的数据安全问题，开发更加高效的分布式安全存储和访问控制技术；三是利用人工智能和机器学习技术实现智能化的访问控制策略管理和安全威胁检测与防御，进一步提高云计算数据的安全性和防护能力，以适应云计算技术发展的需求，为用户提供更加安全可靠的云计算服务。

参考文献：

[1] 章威 . 计算机网络安全存储中云计算技术的作用 [J]. 信息与科技，2018（3）：55.

[2] 梁伟杰 . 基于云计算的计算机实验室网络安全技术研究 [J]. 网络安全技术与应用，2021（12）：64–65.

[3] 巫光福，王影军 . 基于区块链与云 – 边缘计算混合架构的车联网数据安全存储与共享方案 [J]. 计算机应用，2021，41（10）：2885–2892.

[4] 李正君 . 计算机网络安全储存中云计算技术的应用 [J]. 科技资讯，2019，17（23）：4–5.

[5] 张俊 . 云计算技术在计算机网络安全中的应用 [J]. 电子技术，2021，50（01）：120–121.

作者简介：

虞培培 1983 年 2 月 1 日生 女 汉族 上海市人 硕士学历 中级工程师，从事云计算方向研究